INTERNAL REVENUE SERVICE
IRS News Release

Media Relations Office | Washington, D.C. | Media Contact: 202.622.4000
www.IRS.gov/newsroom | Public Contact: 800.829.1040

IRS Warns of E-mail Scam Soliciting Donations to California Wildfire Victims

IR-2007-183, Nov. 2, 2007

WASHINGTON — The Internal Revenue Service today warned taxpayers to be on the lookout for a new e-mail scam that appears to be a solicitation from the IRS and the U.S. government for charitable contributions to victims of the recent Southern California wildfires.

In an effort to appear legitimate, the bogus e-mails include text from an actual speech about the wildfires by a member of the California Assembly.

The scam e-mail urges recipients to click on a link, which then opens what appears to be the IRS Web site but which is, in fact, a fake. An item on the phony Web site urges donations and includes a link that opens a donation form which requests the recipient's personal and financial information.

"People should exercise caution when they receive unsolicited e-mail or e-mail from senders they don't know," said Richard Spires, IRS Deputy Commissioner for Operations Support. "They should avoid opening any attachments or clicking on any links until they can verify the e-mail's legitimacy."

The bogus e-mails appear to be a "phishing" scheme, in which recipients are tricked into providing personal and financial information that can be used to gain access to and steal the e-mail recipient's assets.

The IRS also believes that clicking on the link downloads malware, or malicious software, onto the recipient's computer. The malware will steal passwords and other account information it finds on the victim's computer system and send them to the scamster.

Generally, scamsters use the data they fraudulently obtain to empty the recipient's bank accounts, run up charges on the victim's existing credit cards, apply for new loans, credit cards, services or benefits in the victim's name or even file fraudulent tax returns to obtain refunds rightfully belonging to the victim.

The IRS does not send e-mails soliciting charitable donations. As a rule, the IRS does not send unsolicited e-mails or ask for personal and financial information via e-mail. The IRS never asks people for the PIN numbers, passwords or similar secret access information for their credit card, bank or other financial accounts.

Recipients of the scam e-mail who clicked on any of the links should have their computers checked for malicious software and should monitor their financial accounts for suspicious

activity, taking measures to prevent unauthorized access as necessary. Any unauthorized activity should be reported to law enforcement authorities and to the three major credit companies. More information on how to handle actual or potential identity theft may be found in IRS Publication 4535, Identity Theft Protection and Victim Assistance, available on the IRS Web site. Information is also available on the Federal Trade Commission's identity theft Web site.

Recipients of the scam e-mail can help the IRS shut down this scheme by forwarding the e-mail to an electronic mail box, phishing@irs.gov, using instructions found in "How to Protect Yourself from Suspicious E-Mails or Phishing Schemes" on the genuine IRS Web site, IRS.gov. This mail box was established to receive copies of possibly fraudulent e-mails involving misuse of the IRS name, logo or Web site for investigation.

The IRS and the Treasury Inspector General for Tax Administration (TIGTA) work with the U.S. Computer Emergency Readiness Team (US-CERT) and various Internet service providers and international CERT teams to have the phishing sites taken offline as soon as they are reported.

Since the establishment of the mail box last year, the IRS has received more than 30,000 e-mails from taxpayers reporting almost 600 separate phishing incidents. To date, investigations by TIGTA have identified almost 900 host sites in at least 55 different countries, as well as in the United States.

Recipients of questionable e-mails claiming to come from the IRS may also call TIGTA's toll-free hotline at 1-800-366-4484.

The IRS has come across numerous schemes in which e-mails claim to come from the IRS. More information on these schemes may be found on the genuine IRS Web site, IRS.gov, by entering the term phishing in the search box.

—30—